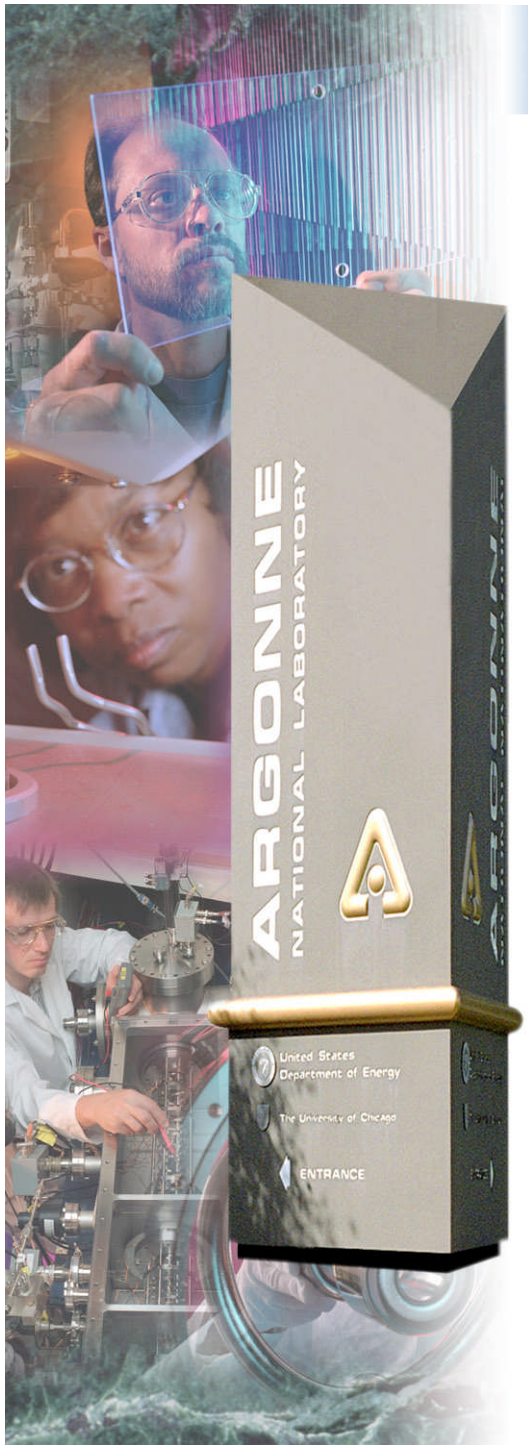


ARGONNE NATIONAL LABORATORY

INFORMATION TECHNOLOGY AT THE APS

Kenneth Sidorowicz

December 13, 2005

THE UNIVERSITY OF CHICAGO

Office of Science
U.S. DEPARTMENT OF ENERGY

Argonne National Laboratory is managed by
The University of Chicago for the U.S. Department of Energy

IT Mission Statement

The mission of the Information Technology Group is to support the strategic goals of the APS, to promote science, and to provide APS access to the latest computer and network technology for the purposes of enhancing science, the operation of the APS, and furthering the goals set by the APS management. To that end, the various responsibilities of the group are as follows:

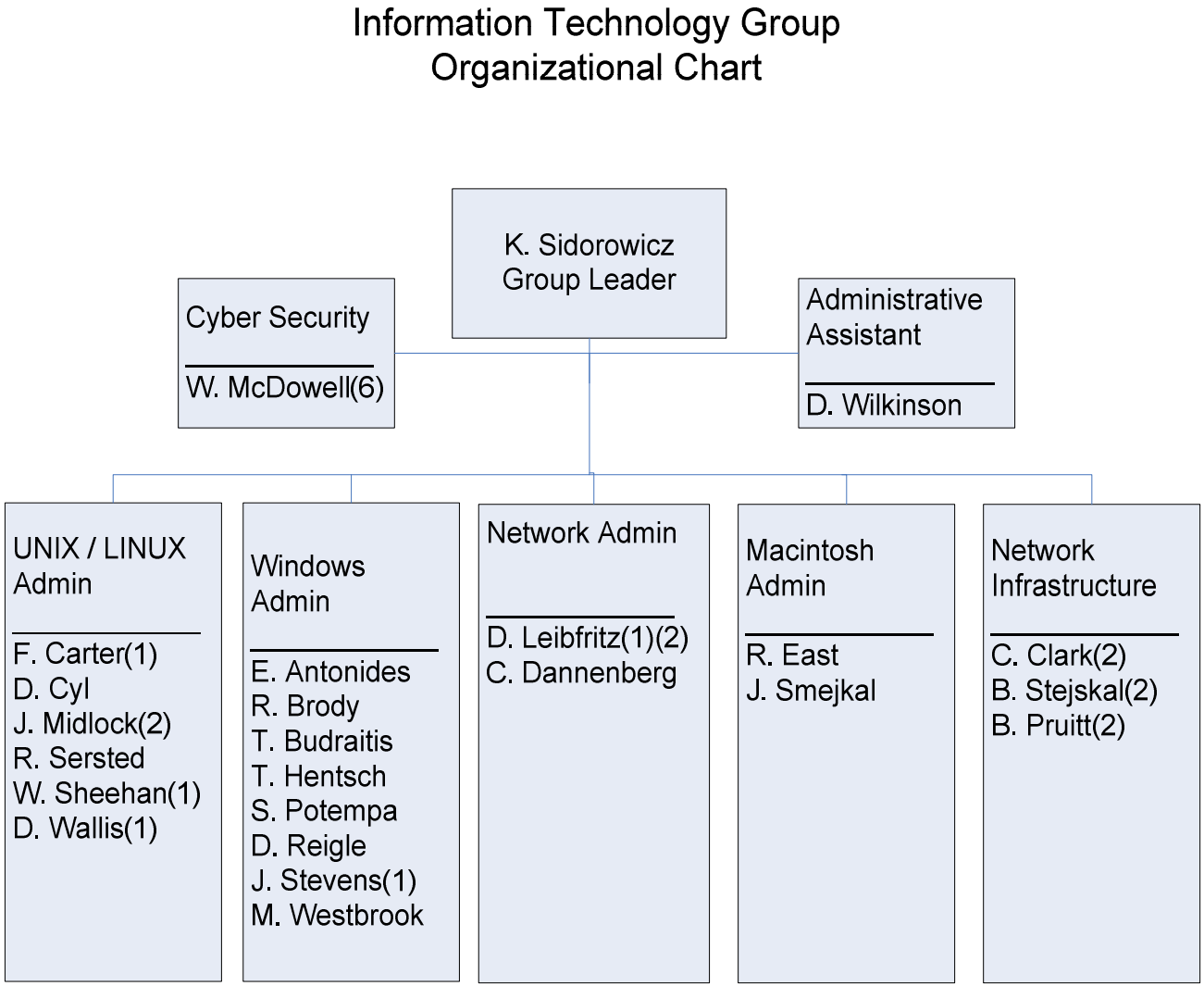
- Set up, maintain and support the APS computer infrastructure including managing all APS Enterprise networks and CAT backbone networks, managing all firewalls, managing computer servers, managing printers, performing tape backups, supporting all Laboratory cyber security policies, managing APS-wide e-mail and various Internet access tools.

- Provide technical support to the APS beamlines in the planning, acquisition, and operation of computers and networking equipment. Scientists do not have to deal with computers and networks, cyber security, backups. They can concentrate on science.

IT Mission Statement

- Provide support for the APS staff in use of software tools and computer technology to be effective and efficient in their work.
- Provide hardware and software support for all APS beamline, accelerator, and central servers and software support for all UNIX, LINUX, Windows, and Macintosh desktop computers.
- Provide software support, including installation of software purchased by and for the performance of Laboratory business.
- Assist in the provision of the transparent integration of technology into the overall APS Mission

Organizational Chart



(1) Beamline Support

(2) Accelerator

(6) STA

Overview of IT Group Responsibilities

- Central computing and networks
  - Includes supporting beamline and accelerator development, and offices in the CLO, EAA and building 412. Building 401 is not a typical office building because offices typically contain control and data acquisition systems being developed for use on the beamlines and accelerator.
  - For the most part there is no separation between applications that operate on the accelerator and beamlines and in the offices and labs of the CLO.
- Networks
  - XOR beamlines, LOMs, Accelerator, Backbone, Central, Argonne Guest House, auditorium and lobby. This includes wired and wireless networks.
- Computers
  - File Servers for XOR beamlines, Accelerator, Central, Argonne Guest House, auditorium and lobby, Web, email, Access Grid, ICMS, CAD, software development, backups, ...
- Cardkey throughout the APS site including APS buildings in the 300 area.

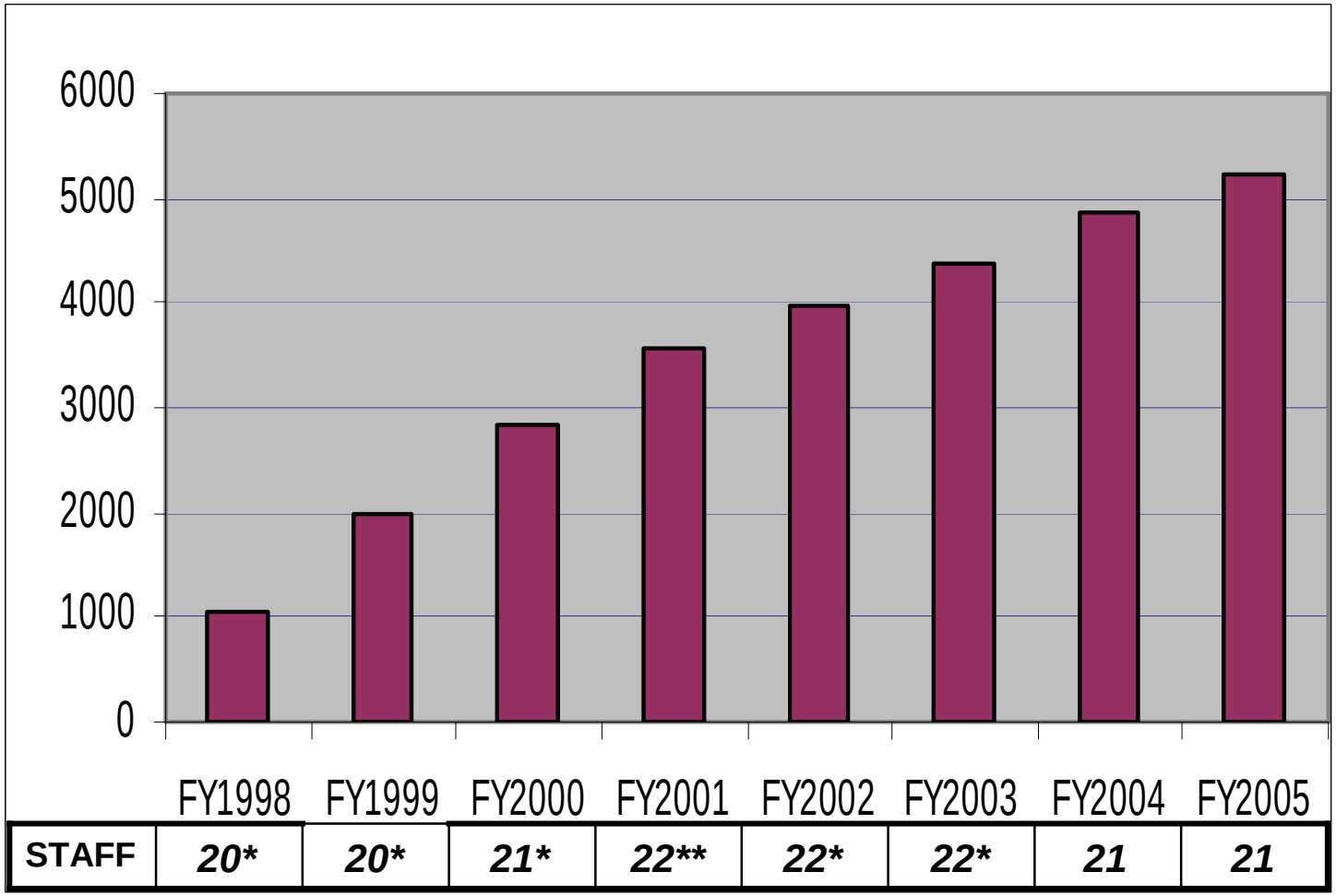
Overview of IT Group Responsibilities cont.

- Conference room projectors
- Video conferencing
  - Capturing conferences and meetings
  - Converting to streaming video for viewing on web
- IITV - Illinois Institute of Technology classes
- CNM computer and network design and support
- All around fix-it shop
  - I have come to the conclusion; if it's in the CLO and has a plug for power, IT is asked to fix it. Yes, even frayed cords on portable vacuum cleaners.

Help Desk Request

Year	Cases
FY1998	1073
FY1999	2000
FY2000	2819
FY2001	3552
FY2002	3976
FY2003	4392
FY2004	4866
FY2005*	5224

*Includes walk-ins, e-mails, and phone calls.



STAFF	*20**	*20**	*21**	*22***	*22**	*22**	*21*	*21*

*Staff included 2 outside consultants working on-site.

**Staff included 3 outside consultants working on-site.

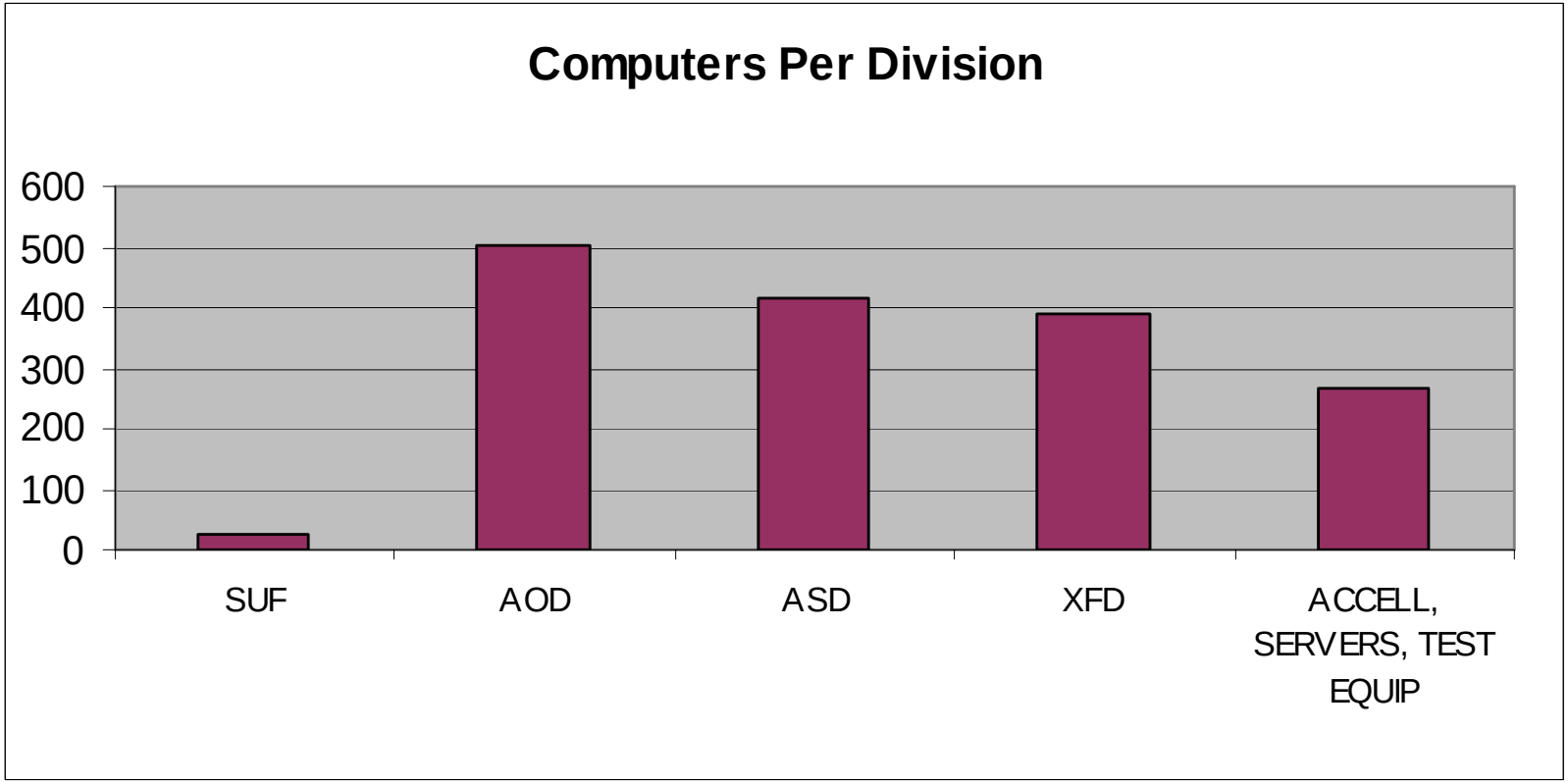
Computer Breakdown per Divisions + Servers

Computer Breakdown per Division

Platform	SUF	AOD	ASD	XFD	ACCELL, SERVERS, TEST EQUIP
Solaris	0	95	91	42	153
Linux	0	67	25	41	10
Windows	20	247	282	178	82
Macintosh	6	93	16	129	23
Total	**26**	**502**	**414**	**390**	**268**

TOTAL APS COMPUTERS

1600



Cyber Security

- DOE Security Tier levels
  - Tier I are defense labs
  - Tier II are labs where secret or classified research can be performed
  - Tier III are labs where no secret or classified research is performed

- Tier I are Sandia, Los Alamos, Lawrence Livermore, Oak Ridge

  Tier II are Argonne, Brookhaven.

  Tier III are Fermilab, JLAB, Berkeley

- DOE cyber security mandates must be implemented with no additional funding. One example is Smart Cards will be required for all computer access. Start date is Oct 1, 2006. All computer users must be using Smart Cards by Oct 1, 2007.

- IT at the Lab is squeezed between DOE orders and maintaining a user-friendly computer environment for the Argonne staff.

Lab IT Committees

- 3.2.2.1 The Information Technology Policy Board (ITPB)

  From the Argonne Cyber Security Program Plan

  - Consists of the chief information officer and representative division directors from each of the associate Laboratory directorates and reports to the Laboratory director.
  - Formulates cyber security policy.
  - Recommends policy to the Laboratory director.
  - Maintains an updated CSPP for the Laboratory.
  - Delegates technical details of policy development and implementation to the Cyber Security Technical Working Group.

- Members — Division
  - Bill Ruzicka — AOD
  - Tom Wolsko — DIS
  - Donald Schmitt — OPS
  - Ray Bair — MCS
  - Remy Evard — CIO/CIS

Lab IT Committees continued

- Information Technology - Architecture Review Group (IT-ARG)

  From the October 3, 2005 Charter Overview

  The Information Technology Architecture and Review Group (ITARG) is responsible for providing guidance, review and recommendations for information technology (IT) changes, handling policy exception requests, and providing technical review of proposed IT policies at the Laboratory. The ITARG is composed of a group of Information Technology experts representing a cross-section of the Laboratory.

IT-ARG Charter

– Reporting

•The ITARG reports to the Information Technology Policy Board (ITPB). It provides an advisory function to the Cyber Security Program Manager (CSPM), Chief Information Officer (CIO) and Information Technology Policy Board (ITPB).

– Membership

Voting Membership of the ITARG shall consist of at least six members, including:

- At least one representative from each of the ANL Associate Lab Directorates (ALD).
- At least one representative from the Cyber Security Program Manager's office.
- At least one current member of the Core Networking Group
- At least two Cyber Security Program Representatives.

In addition, it is a goal that the technical expertise related to both Cyber Security and information Technology of the members be as strong as possible.

The ITARG nominated members who are then approved by the CIO. It is expected that membership will change over time in order to involve many different representatives from across the Laboratory. Members will participate for an average of approximately two years.

IT-ARG Charter

– Responsibility

The ITARG has the following responsibilities:

- To provide an internal peer-review process to validate and comment on:
  - Threat, risk, and vulnerability assessments.
  - System class assessments.
  - Any other assessments performed by Laboratory divisions under the direction of the CSPM.

  These assessments will be advisory to the CSPM.
- To approve or disapprove requested exceptions to Cyber Security policies as defined in the ANL Cyber Security policy and requirements documents and to register these decisions with the CSPM.
- To review the technical implementation of Cyber Security requirements (e.g. firewall rules, password analysis programs, etc) and provide commentary upon such to the CSPM and CIO.
- To act as an advisory board for Information Technology architectural and functional issues at both the Laboratory and the Divisional level, as requested.
- To act as an advisory board for proposed Information Technology and Cyber Security policies at the request of the CIO and IT Policy Board.

IT-ARG committee

Remy Evard	CIO/CIS	Adam Cohen	
MEMBERS	**DIVISION**	**ALD/COO**	
Vito Berardi	ES	Alan Foley	ALD
Paul Domagala	ET/MSD	Alan Foley/Rick Stevens	ALD/CSPR
Mathew Kwiatkowski	IPNS	Murray Gibson	ALD
Gene Rackow	CIS	Adam Cohen	CSPM office
Tracy Rager	DIS	Alan Foley	ALD/CSPR
Dorathea Seymour	DIS	Alan Foley	ALD/CSPR
Kenneth Sidorowicz	APS	Murray Gibson	ALD/CSPR
Michael Skwarek	CIS	Adam Cohen	CSPM Office
John Osudar	CMT	Alan Foley	ALD/CSPR
Scott Pinkerton	CIS	Adam Cohen	Core Networking

Scientific User Facilities	2.0
Physical, Biological, and Computing Sciences	.5
Applied Science and Technology and National Security	4.5
Chief Operating Officer	3.0
Total	**10**

Computer Configuration Management

- From the Argonne Cyber Security Program Plan
  - From a cyber security perspective, it is desirable to have a set of consistent management practices that are uniformly implemented across the organization. This approach has been taken throughout the CSPP and the CSD series. These documents describe configuration management procedures and policies that all ANL organizations must follow, independent of the size and the scope of their computing installations, and where appropriate and possible, to provide centralized resources for policy implementation.

- 6.3 Configuration Management
  - Configuration management is at the core of cyber security. While network protections are critical barriers against external threats, the systems themselves are the last line of defense protecting the data and resources on that system. The quality of the configuration management directly determines the quality of the security protection.
  - The Laboratory's systems are decentralized, with each division being responsible for the configurations of the systems under its control. This situation has the potential to result in variable quality of configuration management across the Laboratory. To address decentralized management, the Laboratory has developed strong configuration management guidance. The guidance that is in place is in the Final CSD Configuration Management documents.
  - The Laboratory has defined a set of base requirements for configuration management, built on top of standards from the Information Technology sector, which all computing installations must meet or exceed in their configuration management.

Configuration Management

- Provides cost savings to the APS
  - Standardizing hardware and software helps to keep IT staff levels down because expertise is not required for multiple vendors hardware or operating systems.
  - Minimizes the number of ghost images and jumpstart/kickstart configurations.
  - Reduces the number of shelf spares.
- Operating systems:
  - Unix - Solaris
  - Linux - Red Hat
  - PC - Windows
  - Macs - OS X
- Hardware:
  - Unix on Suns
  - Linux/Windows on Hewlett Packard desktops and Dell and Hewlett Packard laptops
  - OS X on Macintosh
- Is only effective with continued management support

IT Beamline Support

- Some XOR Beamlines scientists have requested that IT take over management of Linux clusters.
  - Clusters are not always configured properly which makes them not very useful.
  - Scientists don't have the time to install and administer properly.
- XFD management wants all XOR beamlines to be treated the same.
  - IT must now budget for computers and networks for 15 sectors rather than for sectors 1-4 only.
- Beamline computers are "high maintenance" compared to CLO office computers. The beamlines are a very dynamic environment for network and computer operations. Over 3000 users performing experiments with many unique requests to support their beamline equipment.
- Reeducating beamline staff after IT takes over beamline computer and network management.
- IT group needs additional staff to provide first rate and timely support for all XOR beamlines without decreasing support for accelerator or central computing. Budget Proposal # 442 includes 2 engineer positions and 1 technician position for XOR support.
- Budget requests for upgrading networks switches to the standard beamline switches. Managed switches cost more up front but require less staff to maintain.

Beamline Staff Chart

YEAR	STAFF	TOTAL XOR BEAMLINE SECTORS	IT MANAGED XOR SECTORS	IT UNMANAGED XOR SECTORS
1997	2	3	1,2,3	
2000	3	4	1,2,3,4	
2003	4	5	1,2,3,4,8	
2005	4	15	1,2,3,4,8,30,32	6,7,9,11,12,20,33,34
2006	4	15	1,2,3,4,8,9,30,32	6,7,11,12,20,33,34

Future plans

- Reduce server costs by buying workgroup class servers rather than enterprise class and continue to improve performance and maintain a highly available environment.
- Consolidate servers where possible by using Sun's Solaris 10. Zones or virtual systems safely consolidate multiple applications onto a single system to increase utilization rates and cut system and licensing costs.
- Reduce dependence on proprietary operating systems and office applications where possible.
- Improve Linux support for desktops and servers.